

Notice of Allowability

Application No.

09/805,640

Examiner

Kambiz Zand

Applicant(s)

SWILER ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 03/29/2005.
2. ☒ The allowed claim(s) is/are 1-24.
3. ☒ The drawings filed on 13 March 2001 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

DETAILED ACTION

1. The text of those sections of Title 35, U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Petition to the director of USPTO pursuant to 37 C.F.R. 1.181 to invoke supervisory authority have been acknowledged.
4. Claims 1-24 are pending.

Response to Arguments

5. Applicant's arguments filed 03/29/2005 have been fully considered and they are persuasive.

Allowable Subject Matter

6. **Claims 1-24 are allowed.**
7. The following is an examiner's statement of reasons for allowance:

Swiler et al (A Graph-Based Network-Vulnerability Analysis System) teach perform risk and vulnerability analyses of computer networks, examining how an

adversary might be able to exploit identified weakness in order to perform undesirable activities, and assess the universe of undesirable activities that an adversary could accomplish given that they were able to enter the network using an identified weakness. It considers the physical network topology in conjunction with the set of attacks using an attack graph where each node in the graph represents a possible point of attack. It further disclose attack paths using the shortest-path algorithm using canonical representation for all epsilon-optimal paths in order to generate all paths that are no more than epsilon larger than the shortest paths.

Swiler et al's system and method singly or in combination are in contrast with specific steps of applicant's invention where assigning a Length value, L corresponding to a metric reflecting at least one security significant condition bearing on Likelihood of success of an attacker attempting to effect said transition from the start condition, through intermediate conditions, if any, to the end condition, so that the value of L correlates inversely with said Likelihood of success; identifying within said set of paths at Least one shortest path defined as that having the smallest Length value of paths in the set of paths; identifying, from within the set of paths, specific paths having a Length, $L \leq (1+\epsilon)$ times the Length of the shortest path, where ϵ is a non-negative number that accounts for uncertainty in individual edge metric and uncertainty in the actual path the attackers will choose; and designating "epsilon optimal paths" as high risk attack paths as recited in **independent claims 1 and 12.**

8. Dependent claims 2-11 and 13-24 as being dependent upon Independent claim 1 and 12 and having additional allowable features therein.

Conclusion

9. Any comments considered necessary by the applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "comments on statement of reasons for allowance."

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally be reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private

Art Unit: 2132

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197
(toll-free).

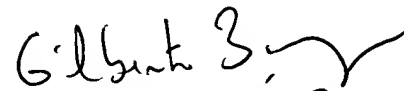
KZ

Kambiz Zand

08/30/2005

AU 2132

571-272-3811



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100